



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,178	08/21/2003	James Edward Bostick	AUS920030362US1	7315

50170 7590 03/19/2007

IBM CORP. (WIP)  
c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.  
P.O. BOX 832745  
RICHARDSON, TX 75083

EXAMINER
----------

WILLIAMS, KENT L

ART UNIT	PAPER NUMBER
----------	--------------

2139

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/19/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/645,178	<b>Applicant(s)</b> BOSTICK ET AL.	
	<b>Examiner</b> Kent L. Williams	<b>Art Unit</b> 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 22 August 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 August 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date: _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>22 August 2003</u> .  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Drawings***

1. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 20-31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

35 U.S.C. 112, sixth paragraph states that a claim limitation expressed in means-plus-function language "shall be construed to cover the corresponding structure...described in the specification and equivalents thereof." "If one employs means plus function language in a claim, one must set forth in the specification an adequate disclosure showing what is meant by that language. If an applicant fails to set

Art Unit: 2139

forth an adequate disclosure, the applicant has in effect failed to particularly point out and distinctly claim the invention as required by the second paragraph of section 112." In re Donaldson Co., 16 F.3d 1189, 1195, 29 USPQ2d 1845, 1850 (Fed. Cir. 1994) (in banc). In summary, one of ordinary skill in the art would not understand what *structure* corresponds to the claimed function(s) of the respective claims. More specifically, "means for automatically logging in," "means for creating said token," "means for establishing a relationship and access level," etcetera, are all not covered by the **structures** presented in the specification **or** one of ordinary skill in the art would not understand which **structure** corresponds to each individually claimed function. Please note the list given is not exhaustive, but merely exemplary. Claims 20-31 that recite "means for" with a function do not have a corresponding *definite* structure within the specification. The Examiner is interpreting the claims as best understood (in the art) in the following art rejections.

4. Claim 4, 24 and 30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 4: "An application other than merely a security mechanism" makes the scope of the indefinite. One having ordinary skill in the art would not know how to interpret the claim. "Security mechanism" is not defined, nor is anything beyond it defined (represented by "other than merely"). Claim 24 and 30: "could represent" is indefinite.

***Claim Rejections - 35 USC § 101***

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 26-31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed towards a "computer-usable medium," which is further defined by the applicants' specification as "any carrier wave, signal or transmission facility" that is non-statutory subject matter. The "computer-usable medium" is further defined as "having computer-executable instructions" that is not to say computer-executable instructions stored on a computer accessible medium *for making the prior-art processor perform* a certain method.

***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1 and 4-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Gupta et al. (U.S. Patent Application Publication No. 2001/0037469 A1).

**Claim 1.** A method for permitting access to applications, said method comprising:  
registering a first restricted application with at least one additional restricted application;  
and in response to a user performing only a single sign-on for said first restricted

application, providing access to said first restricted application for said user [¶0071; login server is synonymous with 'first application server.']; presenting to said user information identifying said at least one additional restricted application; and in response to said user's selection, providing access to said at least one additional restricted application [¶0073; which is an automated process in one embodiment.].

**Claim 4.** The method of Claim 1 wherein: said first restricted application is an application other than merely a security mechanism [¶0067-¶0068; The login server (or 'the first application server') will not be dedicated as such, and will be 'other than merely a security mechanism.'].]

**Claim 5.** The method of Claim 1 wherein: no additional key repository is required by said restricted applications [¶0071; Updating *only* the login server (or 'first application server') is to say only the 'server' is updates, and not a database or 'key repository.'].]

**Claim 6.** The method of Claim 1 wherein: said presenting further comprises said first restricted application sending a document in hypertext markup language [¶0076; URL is inherently HTML.].]

**Claim 7.** The method of Claim 1, wherein said user's selection further comprises: receiving via said first restricted application a selection signal from said user; and in response to said selection signal, sending via said first restricted application a request for access to said at least one additional restricted application [¶0073].]

**Claim 8.** The method of Claim 7, wherein: said user clicks a mouse button when a cursor is positioned over a predefined area of said presented information, to produce said selection signal [¶0073].]

**Claim 9.** The method of Claim 1, further comprising: collecting stored information regarding a user and an appropriate level of access [¶0080]; and sending to said user: a token and a redirect URL pointing to said at least one additional restricted application [¶0076].

**Claim 10.** The method of Claim 9, wherein: said token is encrypted; and said token represents said appropriate level of access [¶0086 and ¶0078].

**Claim 11.** The method of Claim 1, wherein: one of said restricted applications is an intranet web server [¶0071].

**Claim 12.** The method of Claim 1, wherein: one of said restricted applications is a portal [¶0071].

**Claim 13.** The method of Claim 1, wherein: one of said restricted applications is a web application [¶0071].

**Claim 14.** A method for permitting access to applications, said method comprising: registering a first restricted application with a second restricted application [¶0072; In order for the application server and logion server (second and first application servers, respectively, they must have prior knowledge of each other, which is to say they are 'registered' with each other.]; and in response to a user: signing on to said first restricted application only, and requesting access to said second restricted application, automatically logging in to said second restricted application, for said user [¶0076-¶0077; Please note 'without any interaction from the user.']; wherein: no new key repository is required by said first and second restricted applications [¶0071; Updating

*only* the login server (or 'first application server') is to say only the 'server' is updates, and not a database or 'key repository.'].

**Claim 15.** The method of Claim 14, wherein said automatically logging in further comprises: under control of said second restricted application, receiving from said first restricted application, a request to initiate said automatically logging in; sending to said user's client, via said first restricted application a response, having a complete-automatic-log-in URL, and token [¶0076-¶0078]; receiving directly from said user's client a request, having said token; and sending directly to said user's client a response, having authenticated session information [¶0077-¶0079], and a welcome URL [¶0081].

**Claim 16.** The method of Claim 15, further comprising: in response to said request to initiate, creating said token; storing a copy of said token; and associating said token with said request to initiate [¶0078].

**Claim 17.** The method of Claim 15, further comprising: verifying said token received from said user's client; and establishing a relationship and access level for said user's client [¶0078-¶0079].

**Claim 18.** The method of Claim 15 wherein: said token represents an appropriate level of access [¶0079-¶0080].

**Claim 19.** The method of Claim 14, further comprising: under control of said first restricted application, receiving from said user's client a request for access to said second restricted application [¶0073]; in response to said request for access, determining for said user, and said second restricted application, what level of access

should be granted [¶0077]; and sending to said second restricted application a request to initiate said automatically logging in [¶0079].

**Claim 20.** A system for permitting access to applications, said system comprising: means for registering a first restricted application with a second restricted application [¶0072; In order for the application server and logion server (second and first application servers, respectively, they must have prior knowledge of each other, which is to say they are 'registered' with each other.]; and means for automatically logging in to said second restricted application, for a user [¶0078-¶0079]; wherein: no additional key repository is required by said first and second restricted applications [¶0071]; and said means for automatically logging in is responsive to said user: signing on to said first restricted application only, and requesting access to said second restricted application [¶0077-¶0079].

**Claim 21.** The system of Claim 20, wherein said means for automatically logging in further comprises: means for receiving from said first restricted application, a request to initiate said means for automatically logging in [¶0073]; means for sending to said user's client, via said first restricted application, a response, having a complete-automatic-log-in URL, and a token [¶0076]; means for receiving directly from said user's client a request, having said token [¶0076-¶0077]; and means for sending directly to said user's client a response, having authenticated session information [¶0078], and a "welcome" URL or initial URL [¶0081].

Art Unit: 2139

**Claim 22.** The system of Claim 21, further comprising: means for creating said token; means for storing a copy of said token; and means for associating said token with said request to initiate [Figure 1 and ¶0078].

**Claim 23.** The system of Claim 21, further comprising: means for verifying said token received from said user's client [¶0078-¶0079]; and means for establishing a relationship and access level for said user's client [¶0080].

**Claim 24.** The system of Claim 21, wherein: said token could represent an appropriate level of access [¶0078].

**Claim 25.** The system of Claim 20, further comprising: means for receiving from said user's client a request for access to said second restricted application [¶0073]; means for determining for said user, and said second restricted application, what level of access should be granted [¶0077]; and means for sending to said second restricted application a request to initiate said means for automatically logging in [¶0079].

**Claim 26.** A computer-usable medium, having computer-executable instructions for permitting access to applications, said computer-usable medium comprising: means for registering a first restricted application with a second restricted application [¶0072]; and means for automatically logging in to said second restricted application, for a user [¶0076-¶0077; Please note 'without any interaction from the user.']; wherein: no additional key repository is required by said first and second restricted applications [¶0071; Updating *only* the login server (or 'first application server') is to say only the 'server' is updates, and not a database or 'key repository.']; and said means for automatically logging in is responsive to said user: signing on to said first restricted

application only, and requesting access to said second restricted application [¶0076-¶0078].

**Claim 27.** The computer-usable medium of Claim 26, wherein said means for automatically logging in further comprises: means for receiving from said first restricted application, a request to initiate said means for automatically logging in [¶0072 and Figure 1]; means for sending to said user's client, via said first restricted application, a response, having a complete-automatic-log-in URL, and token [¶0077-¶0078 and Figure 1]; means for receiving directly from said user's client a request, having said token [¶0074 and ¶0084]; and means for sending directly to said user's client a response, having authenticated session information [¶0078], and a welcome URL [¶0081].

**Claim 28.** The computer-usable medium of Claim 27, further comprising: means for creating said token [¶0074-¶0078 and Figure 1]; means for storing a copy of said token [¶0074-¶0078 and Figure 1]; and means for associating said token with said request to initiate [¶0074-¶0078 and Figure 1].

**Claim 29.** The computer-usable medium of Claim 27, further comprising: means for verifying said token received from said user's client [¶0078-¶0080]; and means for establishing a relationship and access level for said user's client [¶0078-¶0080].

**Claim 30.** The computer-usable medium of Claim 27, wherein: said token represents an appropriate level of access [¶0078].

**Claim 31.** The computer-usable medium of Claim 26, further comprising: means for receiving from said user's client a request for access to said second restricted application [¶0076-¶0077]; means for determining for said user, and said second

restricted application, what level of access should be granted [¶0078]; and means for sending to said second restricted application a request to initiate said means for automatically logging in [¶0076-¶0078].

The following is supplementary explanation of the rejection above:

Claims 1, 4-9, 11-13, 14-16, 20-22, 26-28 and 30 recite the limitations of “registering” one (claims 14, 20 and 26) or more (claim 1) applications with a “first application” (known in the art as a ‘log-in server’), where a single-sign-on to said first application gives access to it and other “restricted” (web) applications by “information identifying” them and requiring “no additional key repository.” Claims 14, 20 and 26, limited to two restricted applications, further define the automatic procedure for the second restricted application (as it is the only further action possible). Gupta et al. define the aforementioned as one embodiment “externalize[s] the authentication mechanisms from the application servers” or, more simply, another embodiment “comprises a login server that provides the authentication functionality that may be utilized by one or more web application servers (servers on the web that are running an application or maintain information that require user authentication). (¶0071).” It should be noted that Gupta et al. teach that “the application server does not maintain any knowledge regarding authenticating a user but relies on the login server for authentication... [so that] only the login server needs to be updated with a new authentication mechanism. (¶0071).” Updating only the login server (analogous to the “first application server”) is to say that only the “server” is updated, and not an external (or “additional”) database or “key repository.” Gupta et al. further teach, “...The login

Art Unit: 2139

server may be configured to authenticate a user based on the username and password mechanism... (§0077)" and then proceed by transmitting "a cookie (or token)... to the client's browser. (§0078)." Also, "...the application server sends a redirect message (with the login server's URL) back to the client's browser. The redirect message may include *the application's URL, a cookie [or token] for the application, and a temporary identifier*. ...The browser automatically sends a request to the specified URL (e.g., the login server's URL) without *any interaction from the user* long with any existing cookies (or tokens) for the specified URL. (Emphasis added, §0076)." Please note that the aforementioned *is* an automated process. Regarding the user's selection of information identifying restricted applications for providing access thereto: "At step 300, a user makes a URL request (or a network request). For example, the request may be initiated by entering a URL in a browser, clicking on a hyper link in the browser, or forwarded from an HTML form or Applet which is running inside the browser. (§0073)." Regarding the presentation of a "welcome URL" after authentication (claims 15, 21 and 27), such is well known and practiced in the art and would be inherent within the invention of Gupta et al. Please see Figure 3, block 314.

Claims 17-19, 23-25, 29 and 31 recite the limitations as in the previous paragraph and further define "access level" setting during authentication of respective applications. Gupta et al. teach access level setting for specific (web) applications via authentication within their invention as, "...the application server may send the browser's request to an 'authorization service' to check if the user is authorized for the request. The authorization service may then retrieve a profile for the user (e.g., from a

'profile service') and compare the profile to a list of those users that are authorized for the request. (¶0080)."

Claim 10 recites the limitation that the "token is encrypted" and represents "level of access." "Level of access" is shown to be taught within the previous paragraph (the referenced paragraph number eighty, supra). Gupta et al. state, "...The secure communication may provide that any information transmitted is encrypted prior to transmission. [...] One commonly utilized secure protocol that may be utilized by one or more embodiments of the invention is referred to as HTTPS... (¶0086)."

### ***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent Application Publication No. 2001/0037469 A1).

Art Unit: 2139

Claims 2 and 3 further recite the limitations of a single-registration for all authorized users of a restricted application, and “performing a plurality of registrations for a plurality of registrations for a plurality of groups of authorized users of said first restricted application” with “access levels for each group.” The limitations inherited from their parent claims are taught per the 35 U.S.C. 102(b) rejection, *supra*.

Gupta et al. teach the system and method for an automated (and transparent) sign-on process to addition “restricted” applications by use of URL extensions (or tokens) and permissions granted via the sign on of a “first” restricted application (also known as a ‘login server’), as presented in the 35 U.S.C. 102(b) rejection, *supra*. However, Gupta et al. fail to teach said system and method in the plurality (recited as “performing a plurality of registrations” of groups of users). Despite, it would have been obvious at the time the invention was made to one having ordinary skill in the art to include the ability of multiple registrations for respectively multiple users because it has been held that mere duplication of the essential working parts of a device involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ 8. Further, performing a single-sign-on for a group of users is the mere repetition (or duplication thereof) of performing a single-sign-on for a single user (e.g., the process must be *repeated* for all users, even when registering multiple users as a ‘group’).

***Conclusion***

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Royer et al. (U.S. Patent No. 7,143,437 B2) teaches all found within Gupta et al., including much more detail. Please see Figure 2 for more details.

---

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kent L. Williams whose telephone number is 571-270-1376. The examiner can normally be reached on Mon-Fri 7:00-4:30 with Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Williams  
3/13/2007

*Taghi T. Arani*  
*Primary Examiner*  
*Paula D. Arani*  
*3/16/07*